FORM PTO-1390
(REV. 5-93)

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE

ATTORNEY'S DOCKET NUMBER
**2345/153**

# TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/830784

| INTERNATIONAL APPLICATION NO. | INTERNATIONAL FILING DATE | PRIORITY DATE CLAIMED: |
|---|---|---|
| **PCT/EP00/08263** | **24 August 2000 (24.08.00)** | **1 September 1999 (01.09.99)** |

TITLE OF INVENTION
METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

APPLICANT(S) FOR DO/EO/US
Rolf LAKOMY and Joerg SCHWENK

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☐ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.

5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☒ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)

6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).

7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.

8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)) UNSIGNED.
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

**Items 11. to 16. below concern other document(s) or information included:**

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.

13. ☒ A **FIRST** preliminary amendment.
    ☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.

14. ☒ A substitute specification and a marked up version of the substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report and Form PCT/RO/101.

| U.S. APPLICATION NO. if known, see 37 C.F.R.1.5 | INTERNATIONAL APPLICATION NO. | ATTORNEY'S DOCKET NUMBER |
|---|---|---|
| 09/830784 | **PCT/EP00/08263** | **2345/153** |

17. ☒ The following fees are submitted:

| | CALCULATIONS | PTO USE ONLY |
|---|---|---|
| **Basic National Fee (37 CFR 1.492(a)(1)-(5)):** | | |
| Search Report has been prepared by the EPO or JPO ..... $860.00 | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) ..... $690.00 | | |
| No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2)) ..... $710.00 | | |
| Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO ..... $1,000.00 | | |
| International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4) ..... $100.00 | | |
| **ENTER APPROPRIATE BASIC FEE AMOUNT =** | $ 860 | |
| Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(e)). | $ | |

| Claims | Number Filed | Number Extra | Rate | | |
|---|---|---|---|---|---|
| Total Claims | 10 - 20 = | 0 | X $18.00 | $0 | |
| Independent Claims | 2 - 3 = | 0 | X $80.00 | $0 | |
| Multiple dependent claim(s) (if applicable) | | | + $270.00 | $ | |
| **TOTAL OF ABOVE CALCULATIONS =** | | | | $860 | |
| Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must also be filed. (Note 37 CFR 1.9, 1.27, 1.28). | | | | $ | |
| **SUBTOTAL =** | | | | $860 | |
| Processing fee of $130.00 for furnishing the English translation later the ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492(f)). | | | + | $ | |
| **TOTAL NATIONAL FEE =** | | | | $860 | |
| Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). $40.00 per property | | | + | $ | |
| **TOTAL FEES ENCLOSED =** | | | | $860 | |
| | | | | Amount to be refunded: $ | |
| | | | | charged: $ | |

a. ☐ A check in the amount of $_____ to cover the above fees is enclosed.

b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of $860.00 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

**NOTE:** Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288
**CUSTOMER NO. 26646**

Richard L. Mayer

SIGNATURE

Richard L. Mayer, Reg. No. 22,490

NAME

5/1/2001

DATE

Reg. No. 33,865 Aaron C. Dodich

26646

PATENT TRADEMARK OFFICE

[2345/153]

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

| | | |
|---|---|---|
| Applicant(s) | : | Rolf LAKOMY et al. |
| Serial No. | : | To Be Assigned |
| Filed | : | Herewith |
| For | : | METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES |
| Examiner | : | To Be Assigned |
| Art Unit | : | To Be Assigned |

Assistant Commissioner
for Patents
Washington, D.C. 20231

**PRELIMINARY AMENDMENT**

SIR:

Please amend without prejudice the above-identified application before examination, as follows.

**IN THE TITLE:**

Please replace the title with the following:

--METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES--.

**IN THE SPECIFICATION:**

Please amend without prejudice the specification, including abstract, pursuant to the attached substitute specification. Also attached is a marked up version of the substitute specification, in which added text is shaded and in which deleted text is bracketed. No new matter has been added.

EL594612674

**IN THE CLAIMS:**

Without prejudice, please cancel original claims 1 to 4, and please add new claims 5 to 14 as follows:

--5. (New) A method for clearing a customer-specific entitlement in a conditional access system to receive a chargeable service from a service provider by using a security module on which is stored at least one of a security algorithm and the customer-specific entitlement as at least one of a software program and data, the method comprising:

specifically assigning an EMM clearing signal to the security module to provide a specifically assigned EMM clearing signal; and

controlling a right-of-access by a customer through a service center, in response to a request from the service provider to the service center, using the specifically assigned EMM clearing signal by performing one of:

(i) an indirect clearing operation that includes the steps of:

(a) sending the specifically assigned EMM clearing signal from the service center to the service provider via at least one of a telephone system and a data communication system;

(b) feeding the specifically assigned EMM clearing signal for the chargeable service into a control unit of the service provider; and

(c) activating the security module via the control unit by using the specifically assigned EMM clearing signal; and

(ii) a direct clearing operation by sending the specifically assigned EMM clearing signal from the service center, with an assistance of a data transmission service in a digital broadcasting service, to the security module to clear the customer.

6. (New) The method of claim 5, wherein an electronically stored, service-specific credit balance is allocatable in monetary units to the security module.

7. (New) The method of claim 5, wherein in the indirect clearing operation of the security module of a querying customer, the data transmission service is provided by one of a fixed-line modem, a Global System for Mobile Communications (GSM) modem and a GSM-Service Management System (GSM-SMS) modem.

8. (New) The method of claim 5, wherein in the direct clearing operation of the security module of a querying customer:

an approximate location of the querying customer is found with the assistance of at least one of a digital cellular network and a mobile telephony network; and

the specifically assigned EMM clearing signal for clearing the querying customer is only routed into the digital broadcasting network in which the querying customer is situated at a time of a call and an ordering of the specifically assigned EMM clearing signal.

9. (New) The method of claim 5, wherein the chargeable service includes at least one of a pay TV service, a digital radio broadcasting service, a digital video broadcasting service, a service of a Society for Worldwide Interbank Financial Telecommunications and a video-on-demand service.

10. (New) An arrangement for clearing a customer-specific entitlement in a conditional access system to receive a chargeable service from a service provider by using a security module on which is stored at least one of a security algorithm and the customer-specific entitlement as at least one of a software program and data, the arrangement comprising:

an arrangement for specifically assigning an EMM clearing signal to the security module to provide a specifically assigned EMM clearing signal; and

an arrangement for controlling a right-of-access by a customer through a service center, in response to a request from the service provider to the service center, using the specifically assigned EMM clearing signal by performing one of:

(i) an indirect clearing operation that includes the steps of:

(a) sending the specifically assigned EMM clearing signal from the service center to the service provider via at least one of a telephone system and a data communication system;

(b) feeding the specifically assigned EMM clearing signal for the chargeable service into a control unit of the service provider; and

(c) activating the security module via the control unit by using the specifically assigned EMM clearing signal; and

(ii) a direct clearing operation by sending the specifically assigned EMM clearing signal from the service center, with an assistance of a data transmission service in a digital broadcasting service, to the security module to clear the customer.

11. (New) The arrangement of claim 10, wherein an electronically stored, service-specific credit balance is allocatable in monetary units to the security module.

12. (New) The arrangement of claim 10, wherein in the indirect clearing operation of the security module of a querying customer, the data transmission service is provided by one of a fixed-line modem, a Global System for Mobile Communications (GSM) modem and a GSM-Service Management System (GSM-SMS) modem.

13. (New) The arrangement of claim 10, wherein in the direct clearing operation of the security module of a querying customer:

an approximate location of the querying customer is found with the assistance of at least one of a digital cellular network and a mobile telephony network; and

the specifically assigned EMM clearing signal for clearing the querying customer is only routed into the digital broadcasting network in which the querying customer is situated at a time of a call and an ordering of the specifically assigned EMM clearing signal.

14. (New) The arrangement of claim 10, wherein the chargeable service includes at least one of a pay TV service, a digital radio broadcasting service, a digital video broadcasting service, a service of a Society for Worldwide Interbank Financial Telecommunications and a video-on-demand service.--.

## REMARKS

This Preliminary Amendment cancels without prejudice original claims 1 to 4 in the underlying PCT Application No. PCT/EP00/08263, and adds without prejudice new claims 5 to 14. The new claims conform the claims to U.S. Patent and Trademark Office rules and does not add new matter to the application.

The amendments to the specification and abstract reflected in the substitute specification are to conform the specification and abstract to U.S. Patent and Trademark Office rules and to introduce changes made in the underlying PCT application, and do not introduce new matter into the application.

The underlying PCT Application No. PCT/EP00/08263 includes an International Search Report, issued December 22, 2000, a copy of which is included. The Search Report includes a list of documents that were considered by the Examiner in the underlying PCT application.

Applicants assert that the present invention is new, non-obvious, and useful. Prompt consideration and allowance of the claims are respectfully requested.

Respectfully Submitted,

KENYON & KENYON

Dated: 5/1/2001

By: Richard L. Mayer
(Reg. No. 22,490)

By permission of Reg. No. 33,865 for Applicant

One Broadway
New York, NY 10004
(212) 425-7200
(212) 425-5288

**CUSTOMER NO. 26646**

370564v2

# METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

## Field Of The Invention

The present invention is directed to a method for clearing customer-specific entitlements or rights of access in conditional access systems, to receive chargeable services, such as pay TV, digital broadcasting data services in the Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), Society for Worldwide Interbank Financial Telecommunications (SWIFT), video-on-demand, as well as any other digital services broadcast via radio broadcasting systems, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data.

## Background Information

Security modules in the form of smart cards are already in use today in various sectors where people, or machines, need to be granted authorized or conditional access, e.g., conditional access (CA systems), to data, programs, or to other machines, when stipulated conditions or entitlements are satisfied, e.g., pay TV. Other areas of application for smart cards may include electronic payment arrangements, GSM telephony (global system for mobile telecommunications, European digital cellular standard), or digital broadcasting data services in the DAB, DVB, SWIFT, and also, in the future, video-on-demand.

In modern conditional access systems, access is controlled almost exclusively through the use of smart cards that utilize chip card technology. These smart cards may contain stored security algorithms and customer-specific entitlements to receive fee-based data services. In conditional access systems, content providers may encounter the problem of

wanting to reach more than one customer, but not all of them. Only authorized customers should be able to receive a service. These are customers who meet stipulated conditions by purchasing entitlements, for example by paying a monthly subscriber fee. Radio broadcast systems are used to transmit entitlements of this kind. Therefore, it is believed that there is a need to control access to certain information which is disseminated over broadcasting systems, but that, in principle, can be received by everyone.

Conditional access systems, such as pay TV, protect such information from unauthorized access by scrambling, i.e., encrypting the program contents, by storing authorization to receive in the terminal's security module, and by adding receive conditions to the program. The terminals used to receive a pay TV program may include the so-called set-top boxes or decoders. Other types of terminals may include mobile receivers, PC cards, or PCMCIA (Personal Computer Memory Card International Association) modules. The terminal can also be integrated in the television set. In various cases, however, the lack of a way to guarantee receipt may make problematic the clearing of smart cards in broadcast systems, particularly when they are used in mobile devices for receiving services that do not feature point-to-point connections, as telephones do.

A customer cannot utilize a desired service until the card is cleared, immediately following acquisition of the card. However, the sender of a clearing or signal may not have any information on whether his clearing was actually received by the customer. A clearing is not effected when the unit being used is not able to receive a broadcast. This is the case, for example, in underground garages shielded by buildings, or when a radio communications network needed for sending out entitlements is not yet completely built up. In these cases, entitlements, constituted as so-called Entitlement Management Messages (EMM messages), cannot be received on an area-wide

basis. In contrast, a controlled first clearing, including acknowledgment message, can be very reliable and also renders possible an instantaneous collection of charges for the cleared service at the instant of its acquisition.

Program contents are scrambled, in that the data are encoded by an encryption algorithm, with the control of a so-called control word CW. The algorithm mainly used in Europe for digital television based on the MPEG-2 standard (digital code standard of the Moving Picture Expert Group) is the DVB common scrambling algorithm. Other algorithms, however, such as Data Encryption Standard (DES) or triple DES, inter alia, (see Bruce Schneier, Angewandte Kryptographie, [Applied Cryptography], Wiley, 1996) may also be used.

In "Entitlement Control Messages" (ECM), a decoder or other receiver module is not only informed of new control words (CW), but also of the conditions under which a program may be received. Since both the CW, as well as the receive conditions, depend on the particular service, ECMs are allocated to each service. Once an ECM is received, it is directly routed to the security module. The control word CW must be transmitted confidentially. To protect the ECM, cryptographic methods are employed. Since the ECMs are sent to all customers, all authorized customers must possess the same key in order to decode the control word cryptogram. This is referred to as service key SK. The control word CW should be changed at relatively brief intervals, to make it impossible to recognize scrambling patterns.

Entitlement Management Messages (EMM) are used to set and to change receive entitlements stored in the decoder or in the security module. EMM messages must be sent to the individual address of the customer (respectively, of the decoder or of the security module). The customer's address and EMM messages must be protected from change; it must be ensured that only the program provider is able to generate EMM messages.

Individual addresses always appear in the EMM messages as unencrypted messages; piracy protection can only be achieved by using supplementary information that is stored so as to be unreadable for the customer. This is the personal key (PK), which is linked to the customer address. The EMM messages are sent via the same broadcast system as the payload data. The EMM messages are not permanently linked to the program content, but rather to the logical address of the customer's terminal, respectively to that of the security module, so that EMM can be addressed to individual customers or to groups of customers. Moreover, for the use of specific services, such as mobile received services or pay-per-view, a backward channel can be available, which is either implemented manually (call at a service center) or automatically, e.g., connection from the decoder to the transmission center via TCP/IP (Transmission Control Protocol/Internet Protocol).

Entitlements can change when, for example, customers' chargeable accounts are not settled. The consequence of this can be the blocking of a receive authorization, for example. EMMs can also be used, however, for activating or reactivating services on smart carts. In these cases, the entitlements must be reset in the security module, such as the smart cart. Today, as security modules, chip cards are mostly used which are not permanently connected to the terminal, but rather which can be removed from the terminal and replaced. (See, e.g., Bernd Seiler, Taschenbuch der Telekom Praxis, 1996, Schiele & Schön Berlin 1996; Jörg Schwenk, "Conditional Access" or "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?").

Moreover, with the introduction of new transmission media, such as DAB and DVB-T, pay services are gaining in importance for mobile customers, as well. These are customers, who, for example, carry a terminal along with them in their automobile. Here, however, the following problems may arise:

- the data capacity of the services is limited (e.g., DAB, Swift, among other things);
- the receive situation is difficult (e.g., not yet fully developed broadcasting networks or automobiles located in underground garages); or
- a backward channel is normally not available.

Summary Of The Invention

An exemplary method and/or exemplary arrangement of the present invention is directed to providing a method for an authorized customer's chip card to be made individually addressable to facilitate any change in pay services, and/or to further providing that the pay services are serviceable for mobile customers as well.

Detailed Description

An exemplary method and/or exemplary arrangement of the present invention provides that, in response to a request from a service provider, i.e., an institution, such as a T-Point, authorized to issue or sell security modules, to a service center responsible for controlling rights-of-access, e.g., a data service center in the DAB, in the case of indirect clearing, the service center sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in the case of direct clearing, the service center, with the aid of a data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

In the case of a direct clearing, a service on a security

module, such as a smart card, can be cleared by the particular transmission system, such as by using commercial DAB or DVB receivers themselves, or, in the case of an indirect clearing, with the aid of another service, besides the transmitting service. Following payment of the relevant data service fee, the service center assigns the entitlement by implementing a direct or indirect clearing, as mentioned above, via the smart-card specific EMM. A control unit set up at the service provider confirms activation of the security module, for instance of a smart card, for the service in question.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) are allocated in monetary units to the security module.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of indirect clearing of the security module of the querying customer, the data transmission service is believed to be advantageously carried out, e.g., via a fixed-line modem, via a GSM (Global System for Mobile Communications) modem or via GSM-SMS services (where SMS is an acronym for "Service Management System").

In the case of direct clearing of the querying customer's security module, the approximate location of the customer can be found with the assistance of the cellular network, for example, the GSM network, the customer is using. The specific EMM clearing signal for clearing the customer can be routed just within the DAM single-frequency network, where the customer is located at the time of the call and of the ordering of the EMM clearing signal.

An exemplary embodiment and/or exemplary method of the present invention may implement a backward channel using GSM. In this regard, the sequence is described based on the DAB example:

(i) From his or her automobile, via GSM, for example, the customer signals the data service center in the DAB requesting a clearing, for example, for a single data service or for a subscription, or in the case of non-receipt, a clearing, or an allocation of electronic, service-specific credit (tokens) on the smart card.

(ii) In the data service center in the DAB, in collaboration, for example, with a GSM carrier, e.g., T-Mobil, the GSM cell, respectively, in this manner, the DAB single-frequency network that covers a wider area, is determined in which the caller is located at the very moment.

(iii) The relevant EMM is routed, with the clearing, to the DAB single-frequency network where the subscriber is located.

An exemplary embodiment and/or method of the present invention may further provide that there is no need to broadcast EMMs on a country-wide basis, but still only locally in the DAB service areas where the subscriber is also located. It is believed that this makes the data rate required for the EMMs substantially lower. In the case of a call, it is ensured that the caller can also receive the EMM, since, from an established GSM connection, one can infer the possibility of DAP reception. Further, according to an exemplary embodiment and/or exemplary method of the present invention, a backward channel can be provided for new services.

In this context, the EMMs are not sent, for example, over a GSM channel, since this would presuppose a data connection between the mobile telephone and the DAB receiver, which is, however, theoretically conceivable.

The exemplary embodiment and/or exemplary method in accordance with the present invention is believed to have industrial applicability, in particular for clearing customer-specific access entitlements in Conditional Access Systems to enable chargeable media services to be received.

## Abstract Of The Disclosure

A method for clearing customer-specific entitlements in conditional access systems, to receive chargeable media services, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs. In response to a request from a service provider, such as a T-Point or other institution authorized to sell security modules, in an indirect clearing, the service center responsible for controlling entitlements sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, where this EMM clearing signal for the media service in question is fed into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it. In a direct clearing, the service center, with the assistance of a further data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

# METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

## Field [o]Of [t]The Invention

[
]The present invention is directed to a method for clearing customer-specific entitlements []or rights of access in conditional access systems, to receive chargeable[ ] services, such as pay TV, digital broadcasting data services in the [DAB, DVB, Swift]Digital Audio Broadcasting (DAB), Digital Video Broadcasting (DVB), Society for Worldwide Interbank Financial Telecommunications (SWIFT), video-on-demand, as well as any other digital services broadcast via radio broadcasting systems, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data[, according to the definition of the species in Claim 1].

## Background Information[

1
Security modules in the form of smart cards are already in use today in [many]various sectors where people, or machines[ as well], need to be granted authorized or conditional access[ [], e.g., conditional access (CA systems)[]], to data, programs, or to other machines, when stipulated conditions or entitlements are satisfied[ (], e.g., pay TV[)]. Other[ typical] areas of application for smart cards may include electronic payment arrangements, GSM telephony (global system for mobile telecommunications, European digital cellular standard), or digital broadcasting data services in the DAB, DVB, [Swift]SWIFT, and also, in the future, video-on-demand.

In modern conditional access systems, access is controlled almost exclusively through the use of smart cards that utilize

chip card technology. These smart cards may contain stored security algorithms and customer-specific entitlements to receive fee-based[ ] data services. In conditional access systems, content providers may encounter the problem of[ certainly] wanting to reach more than one customer, but not all of them. Only authorized customers should be able to receive a service. These are customers who meet stipulated conditions by purchasing entitlements, for example by paying a monthly subscriber fee. Radio broadcast systems are used to transmit entitlements of this kind. Therefore, it is believed that there is a need to control access to certain information which is disseminated over broadcasting systems, but that, in principle, can be received by everyone.

Conditional access systems, such as pay TV, protect such information from unauthorized access by scrambling, i.e., encrypting the program contents, by storing authorization to receive[ entitlement ]in the terminal's security module, and by adding receive conditions to the program. The terminals [usually ]used to receive a pay TV program [are]may include the so-called set-top boxes or decoders. Other types of terminals [are also possible, such as]may include mobile receivers, PC cards, or PCMCIA[] (Personal Computer Memory Card International Association) modules. The terminal can also be integrated in the television set. In [many]various cases, however, the lack of a way to guarantee receipt [makes]may make problematic the clearing of smart cards[ problematic] in broadcast systems, particularly when they are used in mobile devices for receiving services that do not feature point-to-point connections, as telephones do.[ ]

A customer cannot utilize a desired service until the card is cleared, immediately following acquisition of the card. However, the sender of a clearing or signal [usually does]may not have any information on whether his clearing[ ]was actually received by the customer. A clearing is not effected

when the unit being used is not able to receive a broadcast. This is the case, for example, in underground garages shielded by buildings, or when a radio communications network needed for sending out entitlements is not yet completely built up. In these cases, entitlements, constituted as so-called [EMM messages (]Entitlement Management Messages (EMM messages), cannot be received on an area-wide basis. In contrast, a controlled first clearing, including acknowledgment message, [is]can be very reliable and also renders possible an instantaneous collection of charges for the cleared service at the instant of its acquisition.

Program contents are scrambled, in that the data are encoded by an encryption algorithm, with the control of a so-called control word CW. The algorithm mainly used in Europe for digital television based on the MPEG-2 standard[] (digital code standard of the Moving Picture Expert Group) is the DVB common scrambling algorithm. Other algorithms[ are also possible], however, such as Data Encryption Standard (DES) or triple DES, inter alia, (see Bruce Schneier, Angewandte Kryptographie,[] [Applied Cryptography], Wiley, 1996) may also be used.

In [so-called Entitlement]"Entitlement Control Messages" (ECM), a decoder or other receiver module is not only informed of new control words (CW), but also of the conditions under which a program may be received. Since both the CW, as well as the receive conditions, depend on the particular service, ECMs are allocated to each service. Once an ECM is received, it is directly routed to the security module. The control word CW must be transmitted confidentially. To protect the ECM, cryptographic methods are employed. Since the ECMs are sent to all customers, all authorized customers must possess the same key in order to decode the control word cryptogram. This is referred to as service key SK. The control word CW should be changed at relatively brief intervals, to make it impossible

to recognize scrambling patterns.

Entitlement Management Messages (EMM) are used to set and to change receive entitlements stored in the decoder or in the security module. EMM messages must be sent to the individual address of the customer (respectively, of the decoder or of the security module). The customer's address and EMM messages must be protected from change; it must be ensured that only the program provider is able to generate EMM messages. Individual addresses always appear in the EMM messages as unencrypted[ ]messages; piracy protection[ ]can only be achieved by using supplementary information that is stored so as to be unreadable for the customer. This is the personal key (PK), which is linked to the customer address. The EMM messages are sent via the same broadcast system as the payload[ ]data. The EMM messages are not permanently linked to the program content, but rather to the logical address of the customer's terminal, respectively to that of the security module, so that EMM can be addressed to individual customers or to groups of customers. Moreover, for the use of specific services, such as mobile received services or pay-per-view, a backward channel can be available, which is either implemented manually (call at a service center) or automatically[ (]; e.g., connection from the decoder to the transmission center via TCP/IP[](Transmission Control Protocol/Internet Protocol).

Entitlements can change when, for example, customers[']' chargeable accounts are not settled. The consequence of this can be the blocking of a receive authorization, for example. EMMs can also be used, however, for activating or reactivating services on smart carts. In these cases, the entitlements must be reset in the security module, such as the smart cart. Today, as security modules, chip cards are mostly used which are not permanently connected to the terminal, but rather which can be removed from the terminal and replaced.[

Reference is made to the related art publication in Bernd Seiler (publisher): taschenbuch der telekom praxis,] (See, e.g., Bernd Seiler, Taschenbuch der Telekom Praxis, 1996, Schiele & Schön Berlin 1996[,]; Jörg Schwenk[:], "Conditional Access" or "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?"[]).

Moreover, with the introduction of new transmission media, such as DAB and DVB-T, pay services are gaining in importance for mobile customers, as well. These are customers, who, for example, carry a terminal along with them in their automobile. Here, however, the following problems may arise:

- the data capacity of the services is limited (e.g., DAB, Swift, [inter alia]among other things);
- the receive situation is difficult (e.g., not yet fully developed broadcasting networks or automobiles located in underground garages); or
- a backward channel is normally not available.

[Technical Objective

]Summary Of The [object]Invention

An exemplary method and/or exemplary arrangement of the present invention is[, therefore,] directed to [provide]providing a method[ which will make it possible] for an authorized customer's chip card to be made individually addressable to facilitate any change in pay services, [the intention also being]and/or to further providing t[o make]hat the pay services are serviceable for mobile customers as well.

[Summary of the Invention

The object is achieved in]Detailed Description

An exemplary method and/or exemplary arrangement of the present invention provides that, in response to a request from

a service provider, i.e., an institution, such as a T-Point, authorized to issue or sell security modules, to a service center responsible for controlling rights-of-access, e.g., a data service center in the DAB, in the case of indirect clearing, the service center sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in the case of direct clearing, the service center, with the aid of a data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.[ The underlying advantage of the present invention is that, in]

In the case of a direct clearing, a service on a security module, such as a smart card, can be cleared by the particular transmission system, such as by using commercial DAB or DVB receivers themselves, or, in the case of an indirect clearing, with the aid of another service, besides the transmitting service. Following payment of the relevant data service fee, the service center assigns the entitlement by implementing a direct or indirect clearing, as mentioned above, via the smart-card specific EMM. A control unit set up at the service provider confirms activation of the security module, for instance of a smart card, for the service in question.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) [can be advantageously]are allocated in monetary units to the security module.

In another exemplary embodiment and/or exemplary method of the present invention, in the case of indirect clearing of the security module of the querying customer, the data transmission service [can]is believed to be advantageously carried out, e.g., via a fixed-line modem, via a GSM[] (Global System for Mobile Communications) modem or via GSM-SMS services[] (where SMS is an acronym for "Service Management System").

In the case of direct clearing of the querying customer's security module, [it is also beneficial that ]the approximate location of the customer can be found with the assistance of the cellular network, for example, the GSM network, [he or she]the customer is using. The specific EMM clearing signal for clearing the customer can be routed just within the DAM single-frequency network, where the customer is located at the time of the call and of the ordering of the EMM clearing signal.

[In this manner, the objectives mentioned above are achieved through implementation of]An exemplary embodiment and/or exemplary method of the present invention may implement a backward channel using GSM. In this regard, the sequence is described based on the DAB example:

[

1. ] (i) From his or her automobile, via GSM, for example, the customer signals the data service center in the DAB requesting a clearing, for example, for a single data service or for a subscription, or in the case of non-receipt,[ ] a clearing, or an allocation of electronic, service-specific credit (tokens) on the smart card. [

]

[2. ] (ii) In the data service center in the DAB, in collaboration, for example, with a GSM carrier[ (], e.g., T-Mobil[)], the GSM cell[ (], respectively, in this

manner, the DAB single-frequency network that covers a wider area[()], is determined in which the caller is located at the very moment. [

]

[3. ] (iii) The relevant EMM is routed, with the clearing, to the DAB single-frequency network where the subscriber is located.[

]

[The advantages of the]An exemplary embodiment and/or method [in accordance with]of the present invention [can thus be seen, in particular, in]may further provide that there is no need to broadcast EMMs on a country-wide basis, but still only locally in the DAB service areas where the subscriber is also located. [T]It is believed that this makes the data rate required for the EMMs substantially lower. In the case of a call, it is ensured that the caller can also receive the EMM, since, from an established GSM connection, one can infer the possibility of DAP reception. [Another important advantage lies in the fact that] Further, according to an exemplary embodiment and/or exemplary method of the present invention, a backward channel [is]can be provided for new services.

In this context, the EMMs are not sent, for example, over a GSM channel, since this would presuppose a data connection between the mobile telephone and the DAB receiver, which is, however, theoretically conceivable.

[Industrial Applicability

]The exemplary embodiment and/or exemplary method in accordance with the present invention is believed to ha[s]ve industrial applicability, in particular for clearing customer-specific access entitlements in Conditional Access Systems to enable chargeable media services to be received.

[]Abstract [

]Of The [present invention is directed to a]Disclosure

A method for clearing customer-specific entitlements[] in conditional access systems, to receive chargeable media services, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs. In response to a request from a service provider, such as a T-Point or other institution authorized to sell security modules,[

]in an indirect clearing, the service center responsible for controlling entitlements sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, where this EMM clearing signal for the media service in question is fed into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it. [

]In a direct clearing, the service center, with the assistance of a further data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

# METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES

## Field of the Invention

The present invention is directed to a method for clearing customer-specific entitlements in conditional access systems, to receive chargeable services, such as pay TV, digital broadcasting data services in the DAB, DVB, Swift, video-on-demand, as well as any other digital services broadcast via radio broadcasting systems, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data, according to the definition of the species in Claim 1.

## Background Information

Security modules in the form of smart cards are already in use today in many sectors where people, or machines as well, need to be granted authorized or conditional access [conditional access (CA systems)] to data, programs, or to other machines, when stipulated conditions or entitlements are satisfied (e.g., pay TV). Other typical areas of application for smart cards include electronic payment arrangements, GSM telephony, or digital broadcasting data services in the DAB, DVB, Swift, and also, in the future, video-on-demand.

In modern conditional access systems, access is controlled almost exclusively through the use of smart cards that utilize chip card technology. These smart cards contain stored security algorithms and customer-specific entitlements to receive fee-based data services. In conditional access systems, content providers encounter the problem of certainly wanting to reach more than one customer, but not all of them.

Only authorized customers should be able to receive a service. These are customers who meet stipulated conditions by purchasing entitlements, for example by paying a monthly subscriber fee. Radio broadcast systems are used to transmit entitlements of this kind. Therefore, there is a need to control access to certain information which is disseminated over broadcasting systems, but, in principle, can be received by everyone.

Conditional access systems, such as pay TV, protect such information from unauthorized access by scrambling, i.e., encrypting the program contents, by storing receive entitlement in the terminal's security module, and by adding receive conditions to the program. The terminals usually used to receive a pay TV program are the so-called set-top boxes or decoders. Other types of terminals are also possible, such as mobile receivers, PC cards, or PCMCIA modules. The terminal can also be integrated in the television set. In many cases, however, the lack of a way to guarantee receipt makes the clearing of smart cards problematic in broadcast systems, particularly when they are used in mobile devices for receiving services that do not feature point-to-point connections, as telephones do. A customer cannot utilize a desired service until the card is cleared, immediately following acquisition of the card. However, the sender of a clearing usually does not have any information on whether his clearing was actually received by the customer. A clearing is not effected when the unit being used is not able to receive a broadcast. This is the case, for example, in underground garages shielded by buildings, or when a radio communications network needed for sending out entitlements is not yet completely built up. In these cases, entitlements, constituted as so-called EMM messages (Entitlement Management Messages), cannot be received on an area-wide basis. In contrast, a controlled first clearing, including acknowledgment message, is very reliable and also renders possible an instantaneous collection of charges for the cleared service at the instant

of its acquisition.

Program contents are scrambled, in that the data are encoded by an encryption algorithm, with the control of a so-called control word CW. The algorithm mainly used in Europe for digital television based on the MPEG-2 standard is the DVB common scrambling algorithm. Other algorithms are also possible, however, such as DES or triple DES, inter alia (see Bruce Schneier, Angewandte Kryptographie, Wiley, 1996).

In so-called Entitlement Control Messages (ECM), a decoder or other receiver module is not only informed of new control words (CW), but also of the conditions under which a program may be received. Since both the CW, as well as the receive conditions, depend on the particular service, ECMs are allocated to each service. Once an ECM is received, it is directly routed to the security module. The control word CW must be transmitted confidentially. To protect the ECM, cryptographic methods are employed. Since the ECMs are sent to all customers, all authorized customers must possess the same key in order to decode the control word cryptogram. This is referred to as service key SK. The control word CW should be changed at relatively brief intervals, to make it impossible to recognize scrambling patterns.

Entitlement Management Messages (EMM) are used to set and to change receive entitlements stored in the decoder or in the security module. EMM messages must be sent to the individual address of the customer (respectively, of the decoder or of the security module). The customer's address and EMM messages must be protected from change; it must be ensured that only the program provider is able to generate EMM messages. Individual addresses always appear in the EMM messages as unencrypted messages; piracy protection can only be achieved by using supplementary information that is stored so as to be unreadable for the customer. This is the personal key (PK), which is linked to the customer address. EMM messages are sent

via the same broadcast system as the payload data. EMM messages are not permanently linked to the program content, but rather to the logical address of the customer's terminal, respectively to that of the security module, so that EMM can be addressed to individual customers or to groups of customers. Moreover, for the use of specific services, such as mobile received services or pay-per-view, a backward channel can be available, which is either implemented manually (call at a service center) or automatically (e.g., connection from the decoder to the transmission center via TCP/IP).

Entitlements can change when, for example, customers' chargeable accounts are not settled. The consequence of this can be the blocking of a receive authorization, for example. EMMs can also be used, however, for activating or reactivating services on smart carts. In these cases, the entitlements must be reset in the security module, such as the smart cart. Today, as security modules, chip cards are mostly used which are not permanently connected to the terminal, but rather which can be removed from the terminal and replaced.

Reference is made to the related art publication in Bernd Seiler (publisher): taschenbuch der telekom praxis, 1996, Schiele & Schön Berlin 1996, Jörg Schwenk: "Conditional Access" or "Wie kann man den Zugriff auf Rundfunksendungen kontrollieren?".

Moreover, with the introduction of new transmission media, such as DAB and DVB-T, pay services are gaining in importance for mobile customers, as well. These are customers, who, for example, carry a terminal along with them in their automobile. Here, however, the following problems arise:

- the data capacity of the services is limited (e.g., DAB, Swift, inter alia);
- the receive situation is difficult (e.g., not yet fully developed broadcasting networks or automobiles located in

underground garages); or

- a backward channel is normally not available.

Technical Objective

The object of the present invention is, therefore, to provide a method which will make it possible for an authorized customer's chip card to be made individually addressable to facilitate any change in pay services, the intention also being to make the pay services serviceable for mobile customers as well.

Summary of the Invention

The object is achieved in that, in response to a request from a service provider, i.e., an institution, such as a T-Point, authorized to issue or sell security modules, to a service center responsible for controlling rights-of-access, e.g., a data service center in the DAB, in the case of indirect clearing, the service center sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or, in the case of direct clearing, the service center, with the aid of a data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer. The underlying advantage of the present invention is that, in the case of a direct clearing, a service on a security module, such as a smart card, can be cleared by the particular transmission system, such as by using commercial DAB or DVB receivers themselves, or, in the case of an indirect clearing, with the aid of another service, besides

the transmitting service. Following payment of the relevant data service fee, the service center assigns the entitlement by implementing a direct or indirect clearing, as mentioned above, via the smart-card specific EMM. A control unit set up at the service provider confirms activation of the security module, for instance of a smart card, for the service in question.

In the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) can be advantageously allocated in monetary units to the security module.

In the case of indirect clearing of the security module of the querying customer, the data transmission service can be advantageously carried out, e.g., via a fixed-line modem, via a GSM modem or via GSM-SMS services.

In the case of direct clearing of the querying customer's security module, it is also beneficial that the approximate location of the customer can be found with the assistance of the cellular network, for example the GSM network, he or she is using. The specific EMM clearing signal for clearing the customer can be routed just within the DAM single-frequency network, where the customer is located at the time of the call and of the ordering of the EMM clearing signal.

In this manner, the objectives mentioned above are achieved through implementation of a backward channel using GSM. In this regard, the sequence is described based on the DAB example:

1. From his or her automobile, via GSM, for example, the customer signals the data service center in the DAB requesting a clearing, for example, for a single data service or for a subscription, or in the case of non-receipt, a clearing, or an allocation of electronic, service-specific credit (tokens) on the smart card.

2. In the data service center in the DAB, in collaboration, for example, with a GSM carrier (e.g., T-Mobil), the GSM cell (respectively, in this manner, the DAB single-frequency network that covers a wider area) is determined in which the caller is located at the very moment.

3. The relevant EMM is routed, with the clearing, to the DAB single-frequency network where the subscriber is located.

The advantages of the method in accordance with the present invention can thus be seen, in particular, in that there is no need to broadcast EMMs on a country-wide basis, but still only locally in the DAB service areas where the subscriber is also located. This makes the data rate required for the EMMs substantially lower. In the case of a call, it is ensured that the caller can also receive the EMM, since, from an established GSM connection, one can infer the possibility of DAP reception. Another important advantage lies in the fact that a backward channel is provided for new services.

In this context, the EMMs are not sent, for example, over a GSM channel, since this would presuppose a data connection between the mobile telephone and the DAB receiver, which is, however, theoretically conceivable.

Industrial Applicability

The method in accordance with the present invention has industrial applicability, in particular for clearing customer-specific access entitlements in Conditional Access Systems to enable chargeable media services to be received.

What is claimed is:

1. A method for clearing customer-specific entitlements in conditional access systems, to receive chargeable services, such as pay TV, digital data transmitted via radio broadcasting in DAB, DVB, Swift, video-on-demand, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs and data,
wherein, in response to a request from a service provider, i.e., an institution authorized to sell security modules, to a service center responsible for controlling rights-of-access, in an indirect clearing, the service center sends an EMM clearing signal, specifically assigned to this security module, either via the telephone or a data communications system, to the service provider, and, there, feeds this EMM clearing signal for the media service in question into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it, or,
in a direct clearing, the service center, with the assistance of a data transmission service in a digital broadcasting service, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

2. The method as recited in Claim 1,
wherein in the case of direct and indirect clearing, an electronically stored, service-specific credit balance (tokens) can be advantageously allocated in monetary units to the security module.

3. The method as recited in Claim 1,
wherein in the case of indirect clearing of the security module of the querying customer, the data transmission service can optionally be carried out via a fixed-line modem, a GSM modem, or via GSM-SMS services.

4. The method as recited in Claim 1 or 2,
wherein in the case of direct clearing of the security module of the querying customer, the approximate location of the customer is found with the assistance of a digital cellular network, and the specific EMM clearing signal for clearing the customer is only routed into the digital broadcasting network in which the customer is situated at the time of the call and of the ordering of the EMM clearing signal.

Abstract

The present invention is directed to a method for clearing customer-specific entitlements in conditional access systems, to receive chargeable media services, with the use of security modules, such as smart cards, on which security algorithms and/or customer-specific entitlements are stored in the form of software programs. In response to a request from a service provider, such as a T-Point or other institution authorized to sell security modules,
in an indirect clearing, the service center responsible for controlling entitlements sends an EMM clearing signal, specifically allocated to this security module, either via the telephone or a data communications system, to the service provider, where this EMM clearing signal for the media service in question is fed into a control unit of the service provider, and the security module is activated via the control unit by this EMM clearing signal assigned to it.
In a direct clearing, the service center, with the assistance of a further data transmission service in a digital broadcasting service, such as the DAB single-frequency network, transmits the specifically assigned EMM clearing signal to the security module of the customer making the request and clears this customer.

[2345/153]

# DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am an original, first and joint inventor of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR CLEARING CUSTOMER-SPECIFIC ENTITLEMENTS ON SECURITY MODULES IN CONDITIONAL ACCESS SYSTEMS FOR PAY SERVICES**, the specification of which was filed as International Application No. PCT/EP00/08263 on August 24, 2000 and filed as a U.S. application having Serial No. 09/830784 on May 1, 2001.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

## PRIOR FOREIGN APPLICATION(S)

| Number | Country Filed | Day/Month/Year | Priority Claimed Under 35 USC 119 |
|---|---|---|---|
| 199 41 550.1 | Fed. Rep. of Germany | 01 September 1999 | Yes |

3-

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004
CUSTOMER NO. 26646


Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Rolf LAKOMY**

Inventor's Signature: _____

Date: 11.06.2001

Residence: Hagenkamp 306
D-48308 Senden
Federal Republic of Germany DEX

Citizenship: German

Post Office Address: Same as above.

Inventor: **Joerg SCHWENK**

JSW

Inventor's Signature: Jg Schwenk

Date: 19/06/2001

Residence: Suedwestring 27
D-64807 Dieburg
Federal Republic of Germany DEX

Citizenship: German

Post Office Address: Same as above.